Submit the completed PIA to
Privacy's SharePoint Customer Center

IRM Case Management

1. Contact Information

A/GIS/IPS Director

Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Case Management (CM)

(b) Bureau: Information Resource Management

(c) System acronym: CM

(d) iMatrix Asset ID Number: 138490

(e) Reason for performing PIA: Triennial security reauthorization

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
CM versions 2.0 and 3.03 have ATO under ITAB 4315. CM has requested a new ATO for version 4.029.

(c) Describe the purpose of the system:
CM is a multi-channel online environment used for collaboration, process management and approvals. It is a secure flexible platform on which to build custom automation workflows. CM customers are domestic and overseas bureaus/offices at the Department that need business process automation (BPA) to capture and manage information workflows.

CM is deployed in a central location from ESOC which allows users to access the application through a web browser via Department approved networks. The system's administrative functions and data are accessible to only authorized Technical Department personnel. Central administration and the hierarchical organization of CM sites allow for the top-down application and enforcement of security restrictions. Role-based permissions are applied to all CM groups — from the system as a whole down to individual files that are managed by local administrators.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

CM serves as a repository for collaborative information, which may include a variety of information from or about the public and Department workforce employees. The nature and sources of the information gathered depend upon the business needs of individual Department organizations and initiatives as well as the laws and policies governing PII. The following information is an example of what may be collected by CM customers:

- □ First Name
- □ Middle Name
- □ Last Name
- □ Maiden Name
- □ Email Addresses
- □ Title
- □ Phone Number
- □ Date of Birth/Place of Birth
- □ Gender (Male/Female)
- □ U.S. Citizen (Y/N)
- □ Social Security Number (U.S. citizens only)
- □ Passport Number
- □ Passport Issuing Country
- □ Photo
- □ Familial Contact Information
- □ Emergency Contact Information
- □ Biographic Information
- □ Mailing/Physical Addresses

Case Management customers are informed of their responsibility to inform and contact the Privacy Office, if they collect PII, through the IRM Memorandum of Agreements (MOA), Operating Level Agreements (OLA), and Memorandum of Understanding (MOU).

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C 2581 (General Authority of the Secretary of State).

Additional authorities governing the collection of PII by CM customers will be dependent on the functional authority of the office. Customer authority to collect PII will be listed in the Memorandums (MOA, MOU, OLA) collected by CM prior to implementation.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  The covering SORN for each CM application varies by the mission of the office. Information included in the Privacy Act may be hosted on individual bureau site collections. Per CM Rules of Behavior any customer retrieving records by a personal identifier is subject to provisions of the Privacy Act.

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)
If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-07-017-01
- Length of time the information is retained in the system: Three years
- Type of information retained in the system:
  Data collected and maintained by CM serves different purposes for different functional areas throughout the Department. Unless specified by customer policies, regulations, or authorities the retention period for records in CM is three years at which time they will be destroyed in accordance with the Department of States Records Disposition Schedule as approved by the National Archives and Records Administration for Information Resources Management Records, Systems Integration, Domestic Operation Files A-07-017-01.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?
Authorities governing the collection of SSNs by CM applications will be dependent on the functional authority of the office.

(c) How is the information collected?
Information is collected on a voluntary or involuntary basis via web based forms or from a list provided to the Department by designated organizations. Case forms containing SSNs are built in CM with secure custom programing. Department personnel may also enter information from hard copies obtained by the Department. CM also maintains electronic files such as Excel spreadsheets, Word documents or other document types that may be stored within CM digitally.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.
NA

(e) What process is used to determine if the information is accurate?
Accuracy of the information is initially the responsibility of each bureau/office that collects and owns the information and subsequently enters it into CM. In general, incoming information will be reviewed by onsite System Administrators and any inconsistencies are corrected by contacting the individual submitting his or her information.

The customer information collected and maintained by CM can be characterized as work-related contact information and is only of value to the operation in CM for the short period of time when a Case is being processed. CM relies on separate Department of State OpenNet Active Directory (AD) housekeeping activities for some guarantee of accuracy, but also reconfirms accuracy of information received from the AD through the process of interacting with customers.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Maintaining accurate information is the responsibility of each bureau or office using CM. Information is collected for each Case to identify and locate the customer in need of service. CM leverages OpenNet AD information to maintain accuracy for user information.

(g) Does the system use information from commercial sources? Is the information publicly available?
Information collected by CM varies by source for each bureau/office.

(h) Is notice provided to the individual prior to the collection of his or her information?
Individual bureaus/offices will be responsible to inform U.S. citizens via printed materials, disclosures, web pages, mailings, phone calls or email that the information they voluntarily provide will be retained in the system.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

CM Customers and individuals providing information related to requests, cases, complaints or submissions will provide information voluntarily. If users decline to submit the information, they may not be provided with the particular service being requested.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

PII collection is required for Case Management customers to complete their mission at the Department. The system uses PII to collect service requests, issue system access approvals, document Department complaints and track internal Department taskers for multiple functional areas. The least amount of PII is collected in order to accomplish these requests in Case Management.

In addition, the CM Rules of Behavior require users to keep privacy in mind while using the application and have been published on the external customer SharePoint site.

5. Use of information

(a) What is/are the intended use(s) for the information?
The collection and uses of the information are dependent upon the business needs of the bureau/office gathering the data. CM is a business process automation service supporting the Department. Individual information is captured through OpenNet Active Directory and is intended to connect the requestor with the requests in the fulfillment of processes.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
The use of CM is consistent with its design and intent. CM contains information within the specifications of what it was designed for.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
Not applicable

(2) Does the analysis result in new information?
Not applicable

(3) Will the new information be placed in the individual’s record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

CM is a collaborative platform. It is designed to automate/facilitate information sharing within the Department so any office or bureau within the Department might collaborate with any other office or bureau as long as they have a need to know. PII will not be shared externally.

(b) What information will be shared?

Sharing of information varies by the mission of the office within the scope of the Department’s regulations.

(c) What is the purpose for sharing the information?

CM is an automated collaborative system. It is designed to facilitate information sharing within the Department.

(d) The information to be shared is transmitted or disclosed by what methods?

System communications occurs through OpenNet email inside the Department in various formats (MS word, PDFs, Excel, etc.). Customer approved users can also access shared information with limited access read-only user licenses.

(e) What safeguards are in place for each internal or external sharing arrangement?

PII will not be shared externally. Additionally, any internal information sharing is encapsulated within the CM application, which has its own IA approved system controls in place. CM follows the IRM Performance Management offices’ internal clearances and holds current Memorandums of Agreement, Understanding and Operating Level Agreements with customers.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The concern regarding sharing information is that the CM tool can interface with external systems through web exchanges. IRM has addressed this concern by only approving CM to operate with the OpenNet boundary. Any sharing that occurs within the approved OpenNet boundary is specific to CM customer defined needs documented in Memorandums of Understanding and Agreement. Sharing from users is conditional on access based on a legitimate need to perform specific tasks. Users sharing information are to work within the confines of their individual access privileges. All users are informed that unofficial use of Department of State systems for any personal reasons is strictly unauthorized.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Full instructions for accessing and amending PII held by the Department are available on the U.S. Department of State Freedom of Information Act (FOIA) website at http://foia.state.gov/. The site also provides complete information on FOIA, the Privacy Act, and related statutes and policies.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Procedures vary by the mission of the office or bureau using CM. Individuals should contact the office or bureau responsible for the initial collection of their information for redress purposes.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Notification methods vary by the mission of the office or bureau using CM. Individuals should contact the office or bureau responsible for the initial collection of their information for redress purposes.

8. Security Controls

(a) How is the information in the system secured?

CM information is secured through secured ESOC servers. Case Management Configuration Guidelines are based on DS security standards. The security standards dictate the acceptable applications, ports, protocols and services that are authorized to be used on the servers. Case management servers are configured using the Microsoft build guide and are configured to allow the least functionality required for the application to operate correctly in the DoS environment. Changes to the hardware, software, security and configuration are processed through Case Management change control boards.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

CM delegates authority to bureau/office System Administrators to limit access to only those who have an official need to know. Access to IRM Case Management is restricted to cleared Department of State direct hire and contractor employees via role based user access profiles in accordance with the principle of least privilege and separation of duties. CM allows only the four following standard user roles.

1) Standard User: Is for all normal access to CM. This role is the most common with access to add, modify, create and utilize CM functionality.

2) Standard Administrator: Is for Data Group Level admin activities. This user is identified by the customer and the user role is for making minor changes to the customers' fields, statuses and workflow.

3) Standard Master: Full access to System forms. For technical team members to manage customer configurations.

4) Standard Viewer: Read only access. For support users that are not permitted to alter case information.

The system and database administrators are the only users with direct access to the database for performing maintenance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The CM system records field changes in continuous database logging accessible by only CM Technical teams. Customer accessible audit logs are available to each bureau/office and reviewed by local administrators to prevent the misuse of the information in CM.

(d) Explain the privacy training provided to authorized users of the system.

All Department employees, Federal and contractor, are required to complete annual cyber security training and certification as well as PA459 Protecting Personally Identifiable Information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

CM inherits authentication from OpenNet. User access rights to Case Management are further restricted to "least privilege" by restricting user profiles as a function of the Windows domain, system changes can only occur in system Developer studios by technical team members. Customers cannot access or change the audit logs, do not have access rights to update or make changes to operational software, configuration parameters, or change access rights on the operational Case servers.

(f) How were the security measures above influenced by the type of information collected?

Each bureau/office determines what information is collected in CM.

9. Data Access

(a) Who has access to data in the system?

Users are identified for need to know by each bureau/office. Assignment privileges are granted through standard OpenNet Active Directory (AD). Government full-time employees (FTE and Contractors) with clearances and current DS security training credentials are permitted to use Case Management.

System Administrator: Maintains system from Customer site.

System User: Is able to access system functionality and modify or contribute to records in Case Management.

System Viewer: Is able to view system records but not modify or contribute to records in Case Management.

(b) How is access to data in the system determined?

Access is determined by each bureau/office. External to the Department, users cannot access collected data. All access is enforced by user profiles in Active Directory according to the principle of least privilege and concept of separation of duties. Each user session is allocated its own memory and deallocated upon logging out; customer users do not have access to the webserver hard disk resources. Onsite System administrators delineate access to groups and case types under the direction of the Customer.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access to collected data is role based on a need to know basis defined by each bureau/office. Technical back end servers, databases and configurations are restricted to CM technical team members. Groups are broken into individual user groups with specific access to CM consoles and functionality.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Controls to prevent the misuse of data include the CM user Rules of Behavior, role based access defined by individual bureau/office, mandatory cyber security training for all department employees and contractors, privacy training, and the Departments Rules of Behavior for protecting PII.

Case Management has a privileged group called "System Administrators" responsible for overall control of the Application. This group has the ability to change account attributes for users within their customer group. These system admins are responsible for managing the user and systems accounts. This responsibility protects privacy and reduces the risk of unauthorized access and disclosure by establishing, activating, modifying, reviewing, disabling, and removing user accounts in Case Management.

The Case Management system logs and time stamps audit records that meet DS configuration requirements. Events can be obtained through queries of the application on the database. Case management employs multiple digital signatures for user workflows, approvals and case tracking. Individuals’ activities can be filtered and checked in audit logs. The audit records are accessible by Technical team members who have access to the Case Management servers.